Reply to Office Action mailed May 21, 2003

REMARKS

Claims 1-41 are pending. Claims 1, 18, and 29 are independent.

The written description has been amended to supply a U.S. patent number and to correct a typographical error. No new matter has been entered.

Claims 1-6, 10, 11, 13-17, 29-33, 37, 38, 40, and 41 stand rejected under 35 U.S.C. § 102(b) for anticipation by U.S. Patent No. 5,802,518 to Karaev et al. ("Karaev"). Remaining claims 7-9, 12, 18-28, 34-36, and 39 stand rejected under 35 U.S.C. § 103(a) for obviousness over a combination of Karaev and U.S. Patent No. 6,314,425 to Serbinis et al. ("Serbinis"). The anticipation rejections should be reconsidered and withdrawn because Karaev does not disclose all of the elements of the relevant claims. The obviousness rejections cannot stand because Karaev and Serbinis, either alone or in combination, do not support a prima facie case of obviousness.

Applicants' invention relates to authentication of users of electronic information and transaction processing systems, and more specifically to systems and methods for authenticating users of program objects in distributed computing environments based on negotiated security contexts. Applicants' "security context" is a non-forgeable data object containing all the information necessary for stateless trusted computing environment ("TCE") components to govern access and action requests made to protected system resources (processes, program objects, information objects, etc.). The security context enables secure binding of authentication, authorization, action request(s) and response(s). As described on page 3 of the application for example, a security context may be built from a user's logon information and from system authorization information that define the user's access rights to protected on-line applications and electronic information.

Karaev (and Serbinis, for that matter) discloses nothing remotely like Applicants' claimed subject matter that involves a security context. Karaev "provides an electronic information distribution system that allows remote users to receive, access and query information that is stored in electronic form at a central server, called a repository

server". Col. 3, ll. 12-15. Karaev permits a user to access a web server from a different user computer or using a different Internet browser, but Karaev "prevents the user (or other users) from 'concurrently' accessing the web server from more than one computer or Internet browser using the same ID". Col. 3, ll. 62-67. Karaev mentions a secure sign-on procedure, an advanced secure system, a secure web server 4 and secure electronic distribution of documents, but preventing concurrent user log-on is the only security service described in detail in Karaev.

In Karaev (and Serbinis), a user is given a cookie or similar identifier and a last-access time-stamp needed by a document management system to make an access decision as to whether to permit a user to store or retrieve an information object. The user logs on and is given access to appropriate information resources, and the central server retains the user profile to enforce access controls. This is stateful operation. As described in Karaev at col. 26, l. 66 - col. 27, l. 14, the user is redirected by a web server to the central server to complete the secure logon operation. According to col. 8, ll. 50-55, the cookie is used to see if the user is already logged on.

Serbinis states that it uses "access tokens to control a user's access to services offered by an Internet-based document management system, in which the access tokens are derived from random numbers independent of user or resource information, thereby providing for enhanced security of the Internet-based document management system". Col. 3, ll. 50-56. Serbinis is also directed to a stateful architecture when it states that "HTTP sessions are stateless, so information on these sessions must be maintained in databases". Col. 19, ll. 14-15. Moreover, Serbinis's "enhanced security" does not teach use of any form of cryptography, but just that a random number is harder to guess. This, of course, adds nothing to security if intercept or theft is possible, and imposition of an expiration time on use limits only the window of opportunity for compromising the system.

In contrast to Karaev's (and Serbinis's) teaching of merely identifying a user to a system's access control enforcement mechanism, Applicants' methods and systems enable users to participate in transactions that may be implemented in modern distributed, nested, transaction processing systems by different program objects, e.g.,

Reply to Office Action mailed May 21, 2003

applications or subroutines, that are substantially independent, even to the extent of executing on different processor hardware. In Applicants' methods and systems, the log-on and request for use of distributed resources are separated in time and process, with no direct communication taking place between the log-on component and any processing resource. This is achieved with Applicants' "security context", which enables stateless operation. Access decisions are made based on the content of the "security context".

Thus, Karaev describes a many-user/one-central-server, stateful architecture while Applicants claim a many-user/many-servers, -processors, -program-objects, stateless environment. Moreover, Karaev (and Serbinis) give users simple cookies, but Applicants provide users with something much different, security contexts containing equivalent state information not provided by Karaev (or Serbinis). Instead, Karaev (and Serbinis) retain the equivalent state information in its (their) document management system.

In both Karaev and Serbinis, electronic documents are managed with a form of directly associated access control list that today is a common kind of log-on component. Applicants, in contrast, provide security contexts that, once issued, are user-specific passports with appropriate visas that allow users continually to access system resources even if a logon component is unreachable. The security context eliminates the need to maintain a one-to-one relationship between user and process thread. Service requests can routed to any appropriate processing component, even those newly instantiated, which are provided with sufficient information by the security context to determine what, when, and if a user's request for access to system resources should be honored.

Anticipation requires disclosure of all elements of a claim, and in accordance with the MPEP, three criteria must be met to establish a prima facie case of obviousness: the cited documents must teach or suggest all of the claim limitations; there must be some suggestion or motivation, either in the cited documents themselves or in the knowledge generally available to one of ordinary skill in the art, to have combined the

teachings of the cited documents; and there must have been a reasonable expectation that the documents could have been successfully combined.

As explained above, Karaev and the combination of Karaev and Serbinis do not teach all of the claim limitations. Moreover, the cited documents would not have supplied any motivation to combine them as suggested by the Action. Finally, there would have been no reasonable expectation that such complex documents could be successfully combined to yield a working system, which even then would have had to be further modified to obtain Applicants' claimed subject matter.

There are other features of Applicants' claims that are absent from the two cited documents, but it is believed unnecessary to discuss them in detail because the absences already discussed are sufficient to preclude rejection of the claims. Moreover, the particular arrangement of features claimed by Applicants has many advantages that are not provided by Karaev and Serbinis. For example, Applicants' arrangements support dynamically configurable processing environments where resources are instantiated and allocated based on user bandwidth demands.

For these reasons, it is respectfully requested that the anticipation and obviousness rejections of claims 1-41 be reconsidered and withdrawn.

It is believed this application is in condition for allowance and an early Notice of same is earnestly solicited. If any questions remain, the Examiner is invited to phone the undersigned at the below-listed number.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

P.O. Box 1404
Alexandria, Virginia 22313-1404
1 919 941 9240

By: _Michael G. Savage_

Michael G. Savage
Registration No. 32,596

Date: August 21, 2003